Claims

What is claimed:

1. A data processing system for generating a key protection certificate comprising;

   a PSD further comprising a unique device name, cryptography means, data processing means, data storage means and communications means;

   wherein said cryptography means includes an asymmetric key pair generating algorithm, a first securely shared secret key, a second securely shared secret key, symmetric cryptography means, a concatenation algorithm, a message authentication code algorithm, cryptographic seed information, a key protection certificate algorithm and a signing algorithm.

2. The system according to claim 1, wherein at least a portion of said cryptographic seed information is used by said asymmetric key pair generating algorithm to generate at least one asymmetric private key and one asymmetric public key upon receipt of at least one key generation command, said keys being stored in a secure domain.

3. The system according to claim 2, wherein said key protection certificate algorithm, upon receipt of said key generation command, generates a plurality of contextual attributes.

4. The system according to claim 3, wherein at least a portion of said contextual attributes are encrypted using said first shared secret key and said symmetric cryptography means to generate private contextual attributes.

5. The system according to claim 4, wherein the remaining unencrypted of said plurality of said contextual attributes forms public contextual attributes.

6. The system according to claim 5, wherein a signed device name is generated using said unique device name and said asymmetric private key as inputs into said signing algorithm

7. The system according to claim 6, wherein said private contextual attributes, public contextual attributes, signed device name and unique device name are concatenated by said concatenation algorithm, generating a first intermediate result.

8. The system according to claim 7, wherein a message authentication code is generated using said second shared secret key and said first intermediate result as inputs into said message authentication code algorithm, forming a second intermediate result.

9. The system according to claim 8, wherein said first intermediate result and said second intermediate result are concatenated by said concatenation algorithm forming said key protection certificate then stored in said secure domain.

10. The system according to claim 1, wherein said unique device name is an embedded serial number.

11. The system according to claim 10, wherein said unique device name is the result of a cryptographic process using said embedded serial number as a cryptographic seed.

12. The system according to claim 1, wherein said communications means includes means for receiving commands to generate asymmetric and symmetric keys and means for sending said public key and said key protection certificate.

13. A data processing system for validating a key protection certificate comprising;

data processing means, data storage means, communications means, cryptography means, a first securely shared secret symmetric key, a second securely shared secret symmetric key and a public key, wherein the cryptography means includes a message authentication code algorithm, cross referencing means and a comparator algorithm.

14. The system according to claim 13, wherein said first symmetric key, said second symmetric key and said public key have a direct generation relationship with said key protection certificate

15. The system according to claim 13, wherein said communications means includes means for transmitting requests for said key protection certificate and said public key and means for receiving said key protection certificate and said public key.

16. The system according to claim 15, wherein said received key protection certificate includes private contextual attributes, public contextual attributes, a device name, a signed device name and a message authentication code.

17. The system according to claim 16, wherein said device name is used by said cross referencing means for selecting the proper shared secret keys, public key, cryptographic algorithms and reference parameters associated with said key protection certificate.

18. The system according to claim 17, wherein said signed device name is decrypted using said public key, generating a second device name.

19. The system according to claim 18, wherein said second device name and said device name contained in said certificate are compared by the comparator algorithm to determine if said second device name and said device name contained in said certificate match.

20. The system according to claim 16, wherein a second message authentication code is generated using said private contextual attributes, public contextual attributes, device name, said signed device name included in said certificate and said second shared secret key as inputs into said message authentication code algorithm.

21. The system according to claim 20, wherein said second message authentication code and said message authentication code contained in said certificate are compared using said comparator algorithm to determine if said second message authentication code and said message authentication code contained in said certificate match.

22. The system according to claim 16, wherein said private contextual attributes are decrypted using said first shared secret key.

23. The system according to claim 22, wherein at least one predetermined parameter is contained in at least a portion of said decrypted private contextual attributes.

24. The system according to claim 23, wherein at least one predetermined parameter and said reference parameters are compared using said comparator algorithm to determine if said at least one predetermined parameter and said reference parameters match.

25 The system according to claim 19, 21 or 24, wherein a failure to achieve a match invalidates said key protection certificate.

26. A method for generating a key protection certificate comprising;

injecting a first securely shared secret symmetric key, a second securely shared secret symmetric key, a key protection algorithm and cryptographic seed information into a PSD, wherein at least a portion of said seed information is used in generating at least one public key and one private key,

storing said injected symmetric keys and said seed information in a secure domain within said PSD,

sending a command to said PSD for generating said at least one public key and one private key, wherein said command initiates generation of said keys and of said key protection certificate,

generating said at least one public key and said one private key using at least a portion of said seed information,

generating contextual attributes specific to at least the generation of said private key,

encrypting at least a portion of said contextual attributes using said first shared secret key, forming private contextual attributes and public contextual attributes, wherein predetermined parameters are included in said private contextual attributes,

storing said public key and said private key in said secure domain,

generating a digital signature of a unique device name using said private key, concatenating said device name, private contextual attributes, public contextual attributes with said digital signature and generating a first intermediate result,

generating a message authentication code of said first intermediate result using said second shared secret key producing a second intermediate result,

concatenating said first intermediate result with said second intermediate result producing said key protection certificate; and

storing said key protection certificate in said secure domain.

27. A method for validating a key protection certificate comprising;

receiving said key protection certificate and a public key, wherein said certificate contains at least a plain text device name portion, a signed device name portion and cryptogram portion,

cross-referencing said device name with proper shared secret keys, public key, cryptographic algorithms and reference parameters associated with said key protection certificate,

verifying said signed device name portion of said certificate using said public key,

comparing the resulting device name with said device name portion included in said certificate,

independently performing a message authentication code function on said concatenated private contextual attributes, public contextual attributes, device name, and signed device name portions of said certificate using a first of said shared secret keys,

comparing the resulting message authentication code with a method authentication code included in said certificate,

decrypting said private contextual attributes using a second of said shared secret keys, comparing at least a portion of the private contextual attributes to the reference parameters,

validating said certificate if said resulting device name matches said device name contained in said certificate, said independently generated message authentication code matches said message authentication code contained in said certificate and at least a portion of said private contextual attributes matches said reference parameter,

rejecting said certificate if any of said matches is not achieved.

28. The method according to claim 27, wherein said receiving party possesses said securely shared secret keys and said public key.

29. The method according to claim 28, wherein said receiving party is a trusted third party certificate authority.